Hindawi
Science and Technology of Nuclear Installations
Volume 2021, Article ID 4092760, 15 pages
https://doi.org/10.1155/2021/4092760

Research Article

Integrated Security System (ISS) Design and Evaluation for Commercial Nuclear Power Plant

Arafat. H. Hamadah,[1] **Mohamed S. Nagy**,[1] **Hanaa Abou-Gabal**,[1] **and Sayed. A. El Mongy**[2]

[1]*Nuclear and Radiation Engineering Department, Alexandria University, Alexandria, Egypt*
[2]*Nuclear and Radiological Regulatory Authority (ENRRA), Cairo, Egypt*

Correspondence should be addressed to Arafat. H. Hamadah; arafat_hamadah@hotmail.com

Received 18 February 2020; Revised 3 March 2021; Accepted 4 April 2021; Published 11 May 2021

Academic Editor: Arkady Serikov

Physical security system, which is also called physical protection system, is very crucial in the nuclear industry for protecting staff, visitors, buildings, assets, and nuclear materials against theft, sabotage, and harmful activities. Theft of nuclear materials has a major impact on the essence of nuclear safeguards. Sabotage of a nuclear facility could endanger the public at large. Reviewing the published literature, it is found that there are no complete physical security system designs based on an integrated network of electronic devices that are devoted to commercial NPPs. And there is no definite evaluation factor that was set to approve such a system. This paper is an evolving solution to this deficiency by proposing an unpreceded integrated security system design applicable to a commonly structured physical layout of any commercial NPP. This proposal provides comprehensive security coverage for the NPP boundaries employing a high level of integration for all subsystems communicated via an IP data network controlled by central management software. This paper is proposing also testing procedures to be followed to evaluate the proposed design. The security system effectiveness will be calculated using mathematical codes by assuming external intrusion attack scenarios. Attributes of each attack scenario will be numerically introduced to the evaluation software EASI and ASSESS codes developed by Sandia Labs, USA. This paper also proposes a threshold value of such security system effectiveness which should be achieved by the commercial NPP security system to achieve the so-called security license.

1. Introduction

In the nuclear field, physical protection systems are considered as an essential field of research to protect its facilities and activities. Sandia Laboratories were the leader in this field. In 1996, Sandia cooperated with some US institutes by forming work groups to develop research and education in the nuclear security field. As a result of Sandia Laboratories efforts, Mary Lynn Garcia published her first textbook in the year 2000, followed by its 2nd editionin 2008, which is ref. [1] in this paper. The book was the essence of 25 years of Sandia experience and research in the security field. This book and other Sandia publications [2–4] focused on the definitions, detection theory, general concepts, and evaluation methodologies of physical security systems.

SANS Institute, USA, also issued a report in the same arena in 2016 describing how to plan for a security program [5].

IAEA in 2017 published *Handbook of Physical Protection Systems Design for Nuclear Materials and Nuclear Facilities* [6] describing the general methodology of security system design. The book was a part of a long series of IAEA Security publications in this regard such as references [7, 8].

To assess the effectiveness of any security system, Sandia developed analytical codes such as ASSESS and EASI described in reference ([1], p. 272; [9]) to measure quantitatively the effectiveness. Primarily, these codes have been used to evaluate security systems for nuclear research facilities, such as the examples described in references [10, 11] by assuming a single attack scenario against the spent fuel pools or research center in research reactors.

A paper titled "Nuclear Security Assessment of Physical Protection System in Nuclear Power Plants" [12] studied attack scenarios against commercial nuclear power plants (NPPs), by a code called Vensim considering extending the adversary delay time which is one of the important parameters used in the existing paper.

NRC, the US Nuclear Regulatory Commission published also its NPP Security Assessment Guide [13], which recommended accepted ranges for P_E and P_D.

In 2018, a hypothetical nuclear power plant (HNPP) layout has been published in the 27th International IAEA training course [14] to be used as a common base structure for the security system designs**,** which is used in the existing paper as a layout for the designed security system devoted to the commercial NPPs. The HNPP abovementioned had been modified to be analogous to a real layout of a common commercial NPP, 3rd generation, having a natural cooling water source as already published in a manufacturer manual ([15], p. 21). This paper designed a security system to protect the HNPP boundaries and vital area buildings. The NPP layout is studied here to identify the critical intrusion routes as a step to calculate the security effectiveness through different attack scenarios. During the evaluation process, the relations between the security effectiveness factor and its components are analyzed and graphed to propose the necessary improvements required for the security system to achieve the targeted effectiveness.

2. Nuclear Power Plants Threats

NPP's could be exposed to terror attacks which could lead to widespread radioactive contamination. The attack threats are of several general types such as commando-like ground-based attacks on cooling pumps or other equipment which could lead to a reactor core meltdown or widespread scattering of radioactivity. An attack on a reactor's spent fuel pool could also be serious. The release of radioactivity could lead to thousands of short-term deaths and a greater number of long-term fatalities. This paper is concerned about the man-made (human) threats to NPP's generated only from the first two categories of the following major threat sources: (1) civil disobedience (NPP opponents), (2) nuclear terrorism, (3) sabotage by insiders, (4) military attacks, and (5) cyberattacks.

3. Hypothetical Nuclear Power Plant

The IAEA HNPP mentioned in the introduction's last paragraph is a site located on a coastal front with a natural cooling inlet. The site perspective is illustrated in Figure 1 and its map is shown in Figure 2, indicating the controlled area boundaries surrounded by a concrete wall fence guarded by guard towers. Both of the protected and vital zone areas are surrounded by double wire mesh fences which are monitored by CCTV and perimeter intrusion detection systems. The security buildings are located outside the vital zone including the Security Command Center (SCC) (#18 in Figure 2) and Security Response Force building (#20). The vital zone includes the most important buildings such as the reactor containment (#1 in Figure 2), turbine-generator (#2), water treatment plant (#6), control building (#9), fuel building (#13), and emergency safety building (#14). The vital zone and its buildings are considered as the highest security, which are usually the target of any adversary aiming for nuclear sabotage or theft. The vital zone boundary is controlled by the inspection gate (#15).

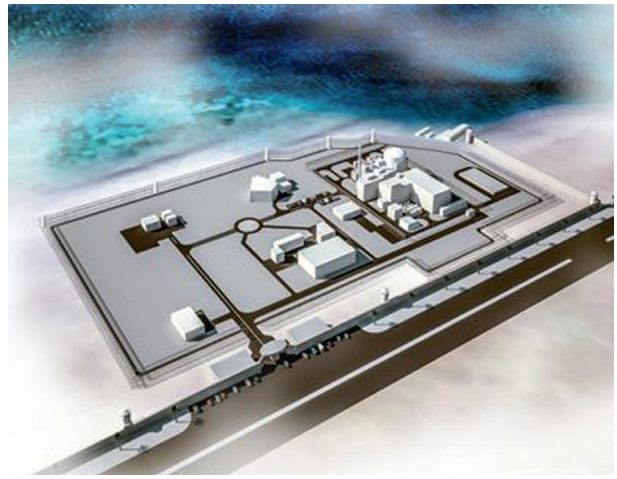

Figure 1: Hypothetical NPP site perspective.

3.1. Security Systems for Concrete Wall Fence. The outside concrete fence is monitored by the Guard Towers described in [16] distributed at every 500 m distance each. Guards direct viewing is essential and is considered as the first detection barrier. The direct naked eyes or using the binoculars are more distinguishing to the real attacks and avoiding false alarms. In most situations, distances between concrete fence and wire mesh fences are short. This is allowing the guards to supervise also the interior mesh fence and is acting as triple verification source for alarms with the intrusion detection and the CCTV systems. Guards are having their communication devices to transfer the data to the Security Command Center (SCC).

Each guard tower is working as a base for PTZ CCTV cameras ([17], p. 22, [18]) specified as a 10 Megapixel IP Camera, 30X Optical Zoom lens with focal length $f = 12.5–375$ mm plus 12X digital zoom to cover a range of 500 m distance according to the lens design tool software [19].

3.2. Security Systems for Double Wire Mesh Fences. The second barrier for the protected area is the double wire mesh fence. The two parallel wire mesh fences are separated by an 8-meter distance. These fences are physical barriers to deter and delay the adversaries. They are monitored by two synchronized electronic systems of automatic detection: the perimeter intrusion detection system [20, 21] and the CCTV system.

The CCTV fixed cameras ([17], p. 7) are installed at every 200 meters, supported by 4–125 mm focal length lenses as calculated by a lens design tool [19]. These outdoor cameras are fixed type; each one is powered by 200-watt solar cells.

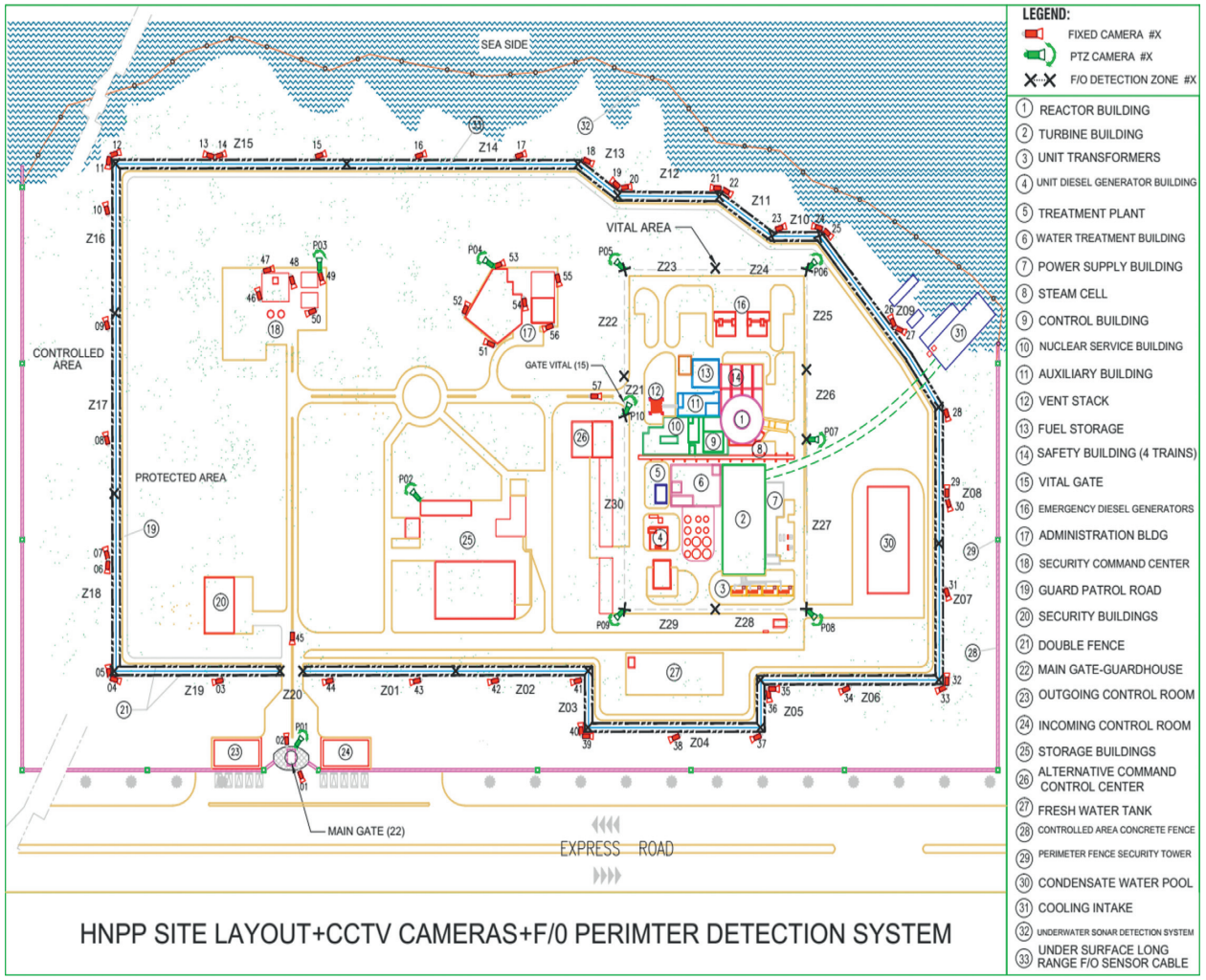

Figure 2: NPP site general location map with CCTV Cameras and F/O Perimeter Detection security distribution.

These cameras are connected to a video server and monitor screens in the SCC ([18], p. 57). The CCTV system is interfaced to the fiber optic intrusion detection system via integrated security system software to follow up any intrusion incidental cases or any activity at the site perimeter ([22], p. 5). All activities are stored in event logs and video records for a period of one year.

The proposed F/O intrusion detection system [20, 21] is composed of fiber cables buried between the two mesh fences linked to a series of transponders connected to the SCC. Each transponder can cover a 20 km range and could be cascaded many times to achieve 80 km of detection range ([21], p. 8]. This range is divided into zones of 200 m each to match with the CCTV camera range.

The F/O detection system supports a cut-immune feature, which enables the system to remain fully operational in the event of a F/O sensor cable cut. The sensor cable incorporates single-mode operation in both double fibers to provide redundancy. The cable is jacketed in an armored case to avoid physical damage. The sensor cable is immune to all forms of electromagnetic energy and intrinsically safe within explosive atmospheres.

3.3. Security System for Seaside. The NPP coastal front boundary is protected by the double wire mesh as shown in Figures 1 and 2, in addition to an immersed marine wire mesh made of plastic polyethylene terephthalate (PET) [22] for protection against coastal underwater hidden intrusions. This marine wire mesh is working as a physical security barrier against diving adversaries.

Additionally, an electronic "underwater sonar detection system" ([23], p. 5) is installed inside the seawater to achieve a detection radius of 5 km for each detector. Each zone has a sonar transceiver which is transmitting the alarm signals to the SCC. The SCC automatically will alert the cameras on the double wire mesh fence at the sea shorefront, direct the PTZ cameras on the guard towers at seafront wing, and alert the ground patrol vehicles as well as sea patrol vessels. This system will support long-range detection for different types of underwater threats such as divers using rebreathing apparatus, scuba divers, and unmanned underwater vehicles (UUVs) as shown in Figure 3. The lower part of Figure 4 illustrates the underwater sonar detection system and its connectivity within the integrated security system for the NPP.

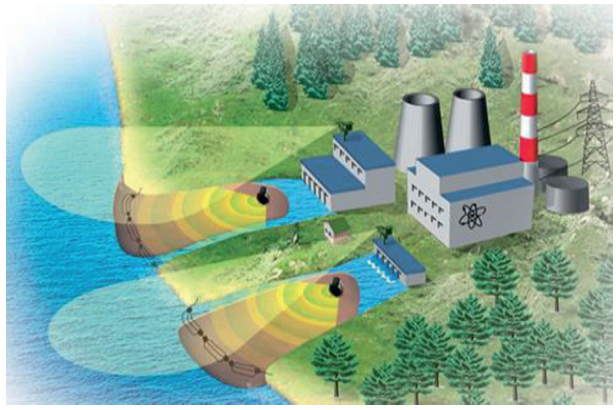

Figure 3: Underwater sonar as part of integrated Security.

3.4. Integrated Security System (ISS) for NPP Boundaries. Figure 4 illustrates the ISS and its following subsystems:

(1) The CCTV system consisting of outdoor fixed cameras and outdoor PTZ cameras.

(2) The F/O perimeter detection system for the outside boundary plus the microwave detection links at gates.

(3) The F/O perimeter detection system for the vital area.

(4) The underwater sonar detection system for the seaside.

Figure 4 illustrates each subsystem component referring to its location by alphabetic addresses. The diagram is also showing the component sequence starting from field sensors passing to the signal coding transmitters via the fiber optic cables necessary for long-distance transmission in such a wide site. All cables are organized in mainframes for data switching via the (IP) data network up to data center servers. Every server carries the management software for each subsystem and its data storage. Finally, all server outputs are monitored on PCs and video wall in the SCC. The effectiveness of the above security system should be tested and evaluated in Section 4.

4. Security System Evaluation

In any NPP, there are many attack targets.

The most critical targets assumed in this study are as follows:

(1) The NPP control building upper floor, specifically the reactor control center (# 9) in Figure 2, which can make the reactor out of control, if it is exposed to sabotage.

(2) The fuel storage building (# 13) in Figure 2, specifically the spent fuel pool and fresh fuel racks that can create radiation accidents due to sabotage, or can create nuclear safeguard problems, if it is exposed to theft [8].

These two buildings are adjacent to each other. The route of attack scenarios, which could be started from different exterior points, most probably will be ending at an in-between common area and then branching to either one of the two buildings as explained in Section 4.1.

It is important to test the effectiveness of the system described in Section 3 against any attack. The main functions of the security system are detection, delay, and response to the attack. Detection is the discovery of an adversary activity. Delay is the slowing down of adversary progress to allow the response to act before the end of the adversary mission. Response is the action taken by the response force to prevent the adversary's success [1].

All the above activities are translated into equations addressing the system effectiveness. The quantitative value of a PPS ability to withstand a possible attack P_E is a component of the general risk (R) resulting from a successful attack ([24], p. 3):

$$R = \left[P_A\left(1 - P_E\right)\right] * C, \tag{1}$$

where P_A is the probability of attack occurrence; $(1 - P_E)$ is the probability of an attack to be successful; P_E is the effectiveness probability of the PPS; and C is the extent of attack consequences.

It is presumed that highly exposed facilities will be subject to a single attack at least. It is only a matter of time; that is, $P_A = 1$.

For a nuclear power station, the successful attack will result in large scale consequences, that is, $C = 1$, the relation will be

$$R = 1 - P_E. \tag{2}$$

The higher the PPS ability to interrupt the attack, the lower the risk. The logic of this equation will be explained further in the forthcoming Section 5.4.

P_E is the maximum likelihood estimator of the Bernoulli discrete probability distribution of a random variable which takes a value of 1 or 0.

In another form, P_E is the product of P_I which is the probability of adversary interruption, and P_N is the probability of adversary neutralization ([25], p. 3):

$$P_E = P_I \times P_N. \tag{3}$$

For security system, P_I is a product of the probability of adversary detection P_D and the probability of alarm communicating to Security Command Center P_C as follows:

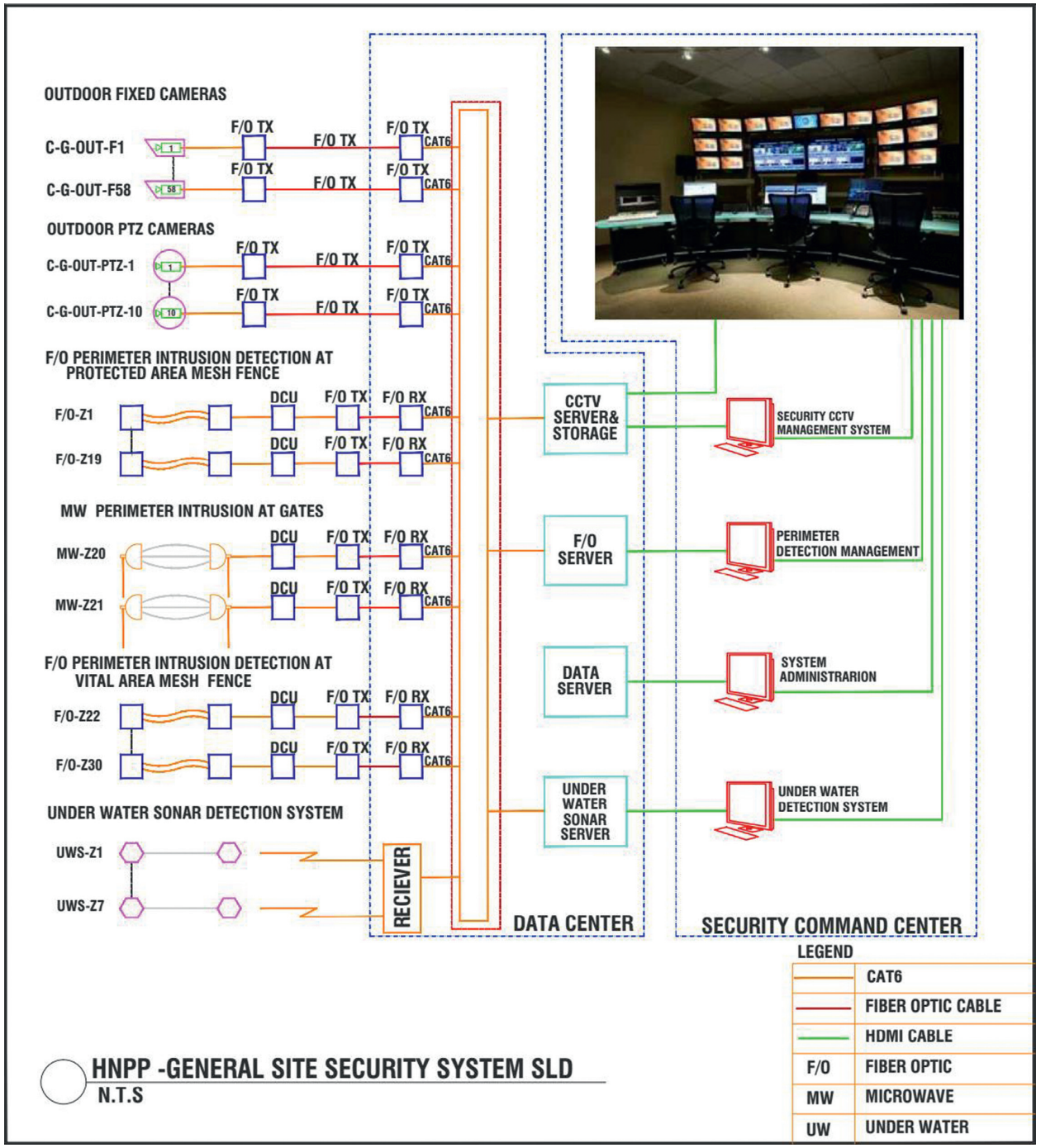

Figure 4: Security system single-line diagram for the NPP boundaries. Cameras and sensors are transmitting their signal to data collection units and via F/O cable and data network to servers in data centers passing to the SCC, alarming PCs and video monitors.

(i) For a single security sensor ([1], p. 276),

$$P_I = P_C \times P_D. \tag{4}$$

Therefore,

$$P_E = P_C \times P_D \times P_N. \tag{5}$$

(ii) For (n) multiple security sensors cascaded on the adversary's path ([1], p. 302; [10] p. 832]:

$$P_I = P_C \times [1 - (1 - P_{D1}) \times (1 - P_{D2}) \times (1 - P_{D3}) \ldots (1 - P_{Dn})]. \tag{6}$$

Equations (4) to (6) are the mathematical bases for EASI code ([1], p. 272) developed to calculate P_I. In the EASI program, input parameters representing the security system functions of detection, delay, and response are required for every specific adversary path and must be fed to EASI input tables, which are as follows:

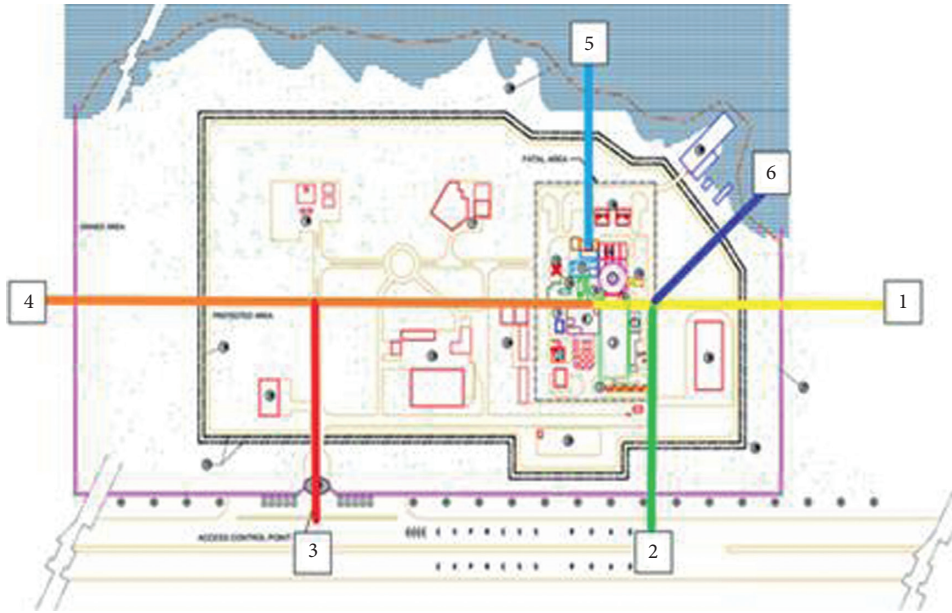

Figure 5: Adversary attack scenarios.

(i) Intruder path sequence scenario (considering terrorist path speed = 4 m/s)

(ii) Detection probability (P_D)

(iii) Delay mean time (MT)

(iv) Delay standard deviations (SD): 30% of the mean value

(v) Response force time (RFT)

(vi) Alarm communication probability (P_C) value should be within the accepted range for the nuclear industry importance, so it will be 0.95 minimum

Probabilities of neutralization P_N in equation (3) can be calculated by using the software called ASSESS Neutralization Code ([1], p. 271). This program is dealing with the adversary threat capabilities and its sophistication as well as the response force capabilities. In practice, neutralization analysis requires threat data and response force data. Threat data include the types and number of adversaries and identification of the specific targets. The information should be collected during the threat definition process. It requires also the response force data containing weapon types, number of guards, transport time, response arrival time, and so forth, for each target.

4.1. Attack and Defense Scenarios. The geographical site conditions of the NPP shown in Figures 1 and 2 were studied to identify the possible attack routes through which adversaries could pass through to execute intentionally planned attacks. A methodology called adversary sequence diagram (ASD) [25], which is a graphical representation used to identify the path elements through protection layers controlling the movement between cascaded areas to identify the paths which adversaries can follow to accomplish their mission. Applying this model to our NPP site, it is found that routes 1, 2, 3, and 4 from the landside and routes 5 and 6 from the seaside can be considered as possible attack routes as shown in Figure 5.

These routes are selected as the most possible routes followed to arrive at the critical targets described above. Route 1 from the landside and route 6 from the seaside are having the shortest distances and the least obstacles which qualify them to be the critical routes. This paper is setting a value of 0.9 as a minimum for the acceptance of P_E based on some examples ([10], p. 835; [13], p. 50; [26], p. 5).

In this paper; attack scenarios are developed in coordination with gradual installation of security surveillance and detection equipment; this is to be sure of the necessity of each security device added to the system. P_E will be calculated for each scenario. In this plan, if the evaluation test after any scenario fails to achieve the minimum P_E value, recommendations should be proposed to enhance the security system and the test should be repeated until the achievement of the accepted P_E value.

4.2. Scenario 1.1: Attack via Route 1 with No Electronic Detection System on the Fence. In this scenario, as a trial, the surveillance on the concrete wall fence, double mesh fence, and vital area fence will depend only on human detection; no electronic detection will be used on these fences. The attack through route 1 having these conditions is called attack scenario 1.1 as a basic scenario which will use the inputs of response force delay time indicated in Table 1, P_N value = 0.995 calculated by ASSESS code shown in Figure 6.

Table 1: Response force delay time RFT for scenario 1.1.

Guards delay time	Sec	Response force delay time	Sec
Alarm communication time	1	Alarm communication time	1
Alarm assessment time	45	Alarm assessment time	45
Communication time to guards	25	Communication time to guards	25
Guards preparation time	15	Response force preparation time	90
Guards travel and deployment time	34	Response force travel time (by vehicles)	120
		On-site deployment time (after travel)	75
	120	Total RFT =	356

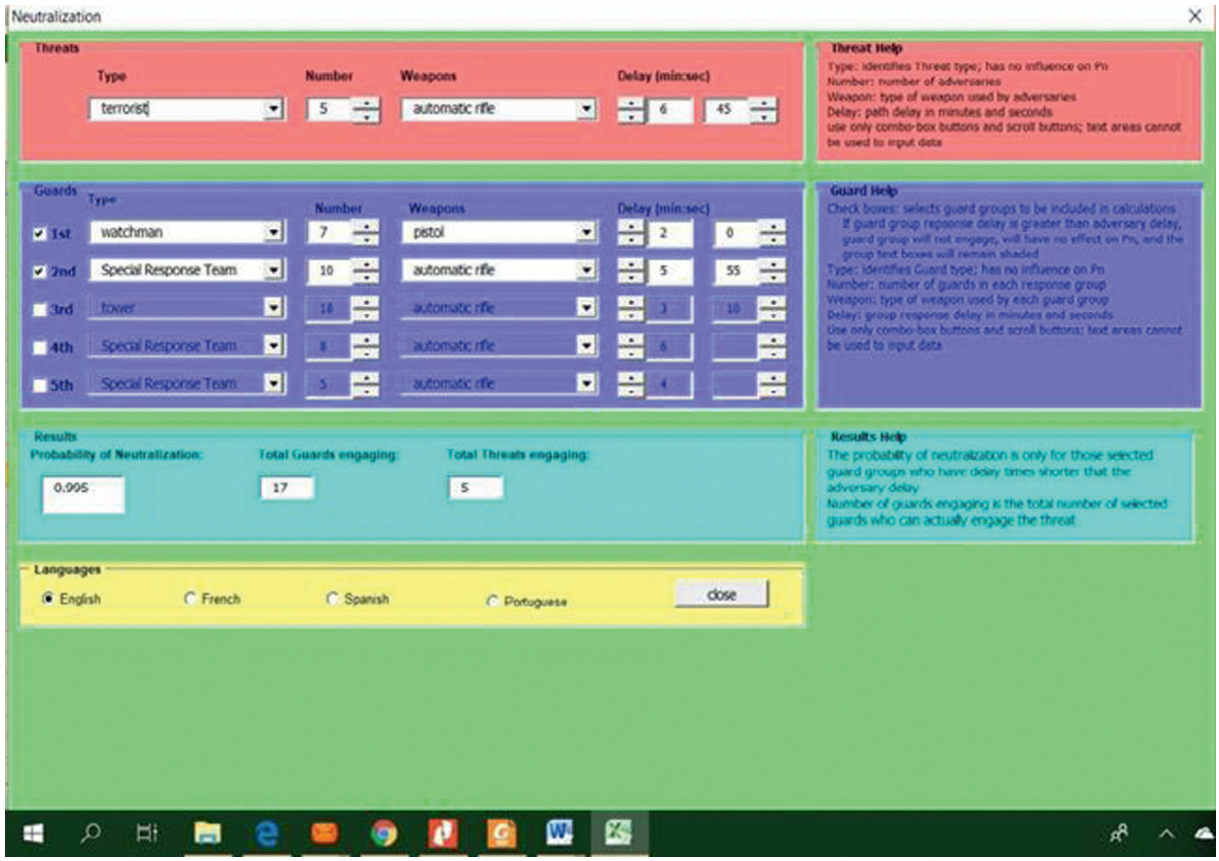

Figure 6: ASSESS code calculation results for the probability of neutralization P_N based on Table 1, response force delay times, and their categories and numbers. The resulting value of $P_N = 0.995$.

Figure 7 shows the attack path action sequence in the description column. The input values for the EASI input sheet are derived from the properties of the security sensors, the delay performed by each barrier, and the RFT values from Table 1.

When the values of RFT, ADT, and P_C of security detection devices as well as P_D of each action along the path of this scenario are introduced to the EASI program, the result is $P_I = 0.00342$ and $P_E = 0.00339$ as in Figure 7 which is extremely low and unacceptable.

4.3. Scenario 1.2: Attack via Route 1 with Electronic Detection System on Fences. P_E evaluation test is failed in scenario 1.1, concluding that human detection of adversaries is not enough. That forces the designer to use electronic surveillance and fence intrusion detection devices on the boundary and vital area fences. P_D of newly added devices will be fed to EASI program in this scenario 1.2 on route number 1. The EASI code for this scenario calculates $P_I = 0.218$ and $P_E = 0.217$, which are still low and unacceptable values.

4.4. Scenario 1.3: Attack via Route 1 with Increasing Adversary Delay Time. In the previous scenario 1.2, P_D was increased to a maximum value based on the addition of surveillance and detection security systems in all intrusion locations, but the P_E resulting value is still very small (0.217) compared to the targeted value of 0.9 or above.

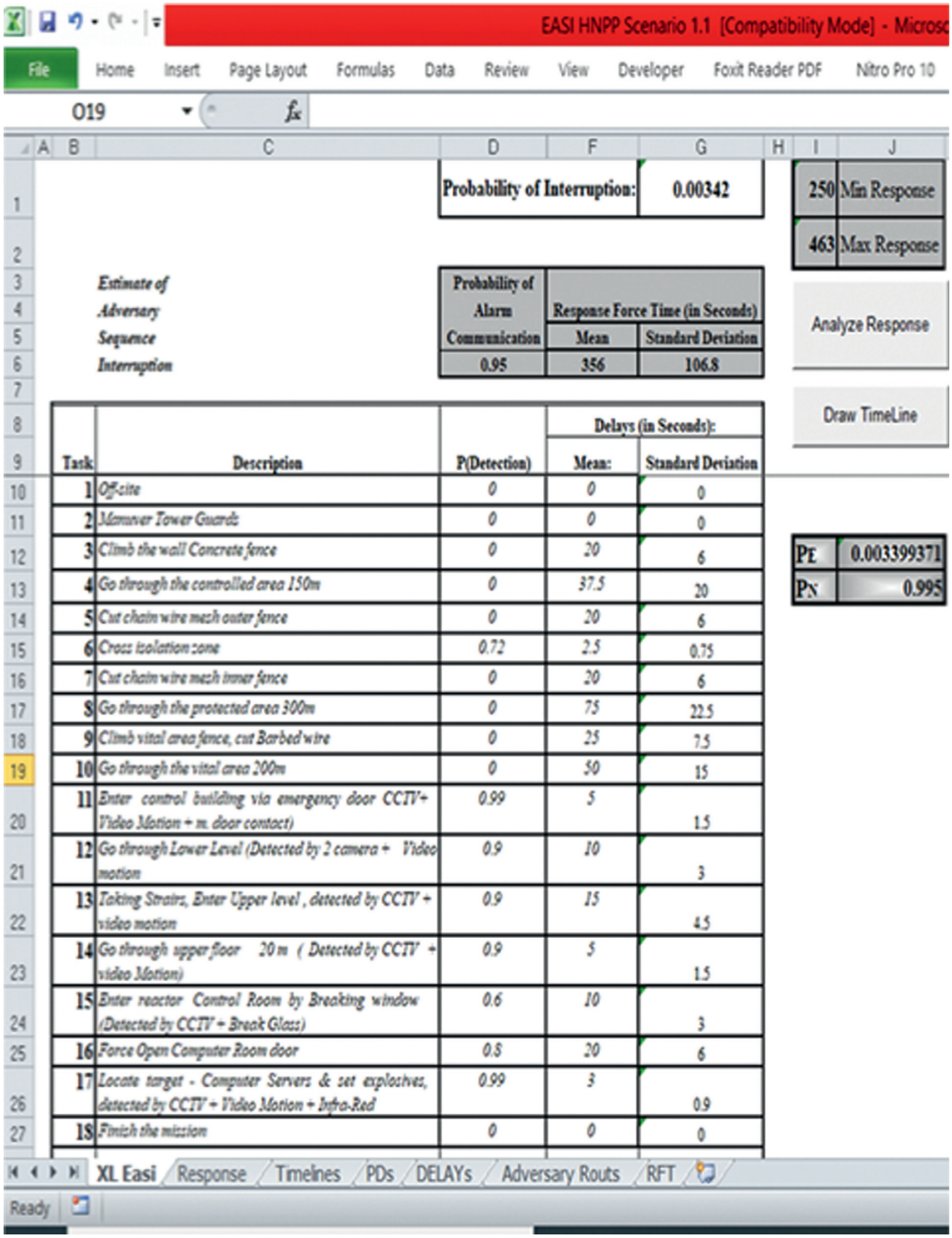

Figure 7: Attack path action sequence and EASI calculations of P_I and P_E for scenario 1.1, which results in $P_E = 0.00339$, are very low and not acceptable.

It is noticed that the total adversary delay time ADT is 298 sec while the total response force time (RFT) is 365 sec. That means although the value of P_D is at its maximum which fulfills the early detection function, the adversaries' mission will be completed before the arrival of the response force. That means there is no way for such a situation to interrupt this mission.

Figure 8 illustrates the tradeoff between ADT and RFT, showing a critical detection point of special importance. If the attack is detected behind this point and adversary delay is not maximized, the response force will not have enough time to act effectively against the adversary ([25], p. 4).

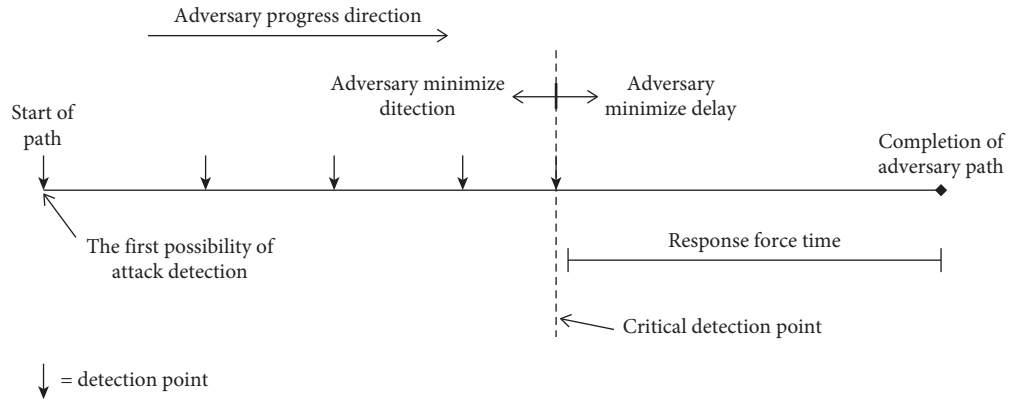

Figure 8: Tradeoff between ADT and RFT and critical detection point [24].

According to the above discovery, it is recommended to increase the ADT and repeat the test in a new scenario 1.3, where the attack will be on the same route number 1, with the following modifications:

(i) Increasing the delay time of the vital area fence by adding blocks of barbed wire rolls behind the first fence side.

(ii) Increasing the delay time required to open the computer room in the control building by manufacturing it from solid steel instead of wood. New ADT values are in green color in tasks 9 and 16 of the EASI code Excel input as shown in Figure 9.

Applying the above recommendations will produce a total ADT = 573 sec compared to 298 sec in scenario 1.2; other inputs to the EASI program will stay the same. These conditions will exercise a new scenario called 1.3 illustrated in Figure 10. The results of EASI code calculations are depending on the max P_D values, ADT total = 573 sec, and the same RFT value of 356 sec as described in Table 1. The calculation is resulting in $P_I = 0.862$ and $P_E = 0.858$. The P_E value has been increased considerably but still less than the targeted 0.9 value. That is requiring additional analysis to determine how to achieve the targeted value of P_E.

These analyses have been graphed in Figure 10 showing the relation between P_I and consequently P_E (as $P_E = P_I \times P_N$) from one side and its component parameters P_D, ADT, and RFT separately from the other side.

Overall, P_D value jumps in steps till arriving to its maximum P_D, contribution in the P_I value; the P_I value stands at 0.865 as a fixed maximum value in spite of any new increase in P_D which means no more upgrades in the security system could gain a higher P_I value. It is not recommended to add security devices as it will add cost with no extra gain.

ADT is making a good contribution to P_I. P_I is increasing in a positive proportionality shape approaching a saturation value of 0.94 at ADT = 500 sec and above, which means no more increase in P_I with the increase of ADT value.

The relation between P_I and RFT is a negative proportionality shape. P_I is increasing with the decrease of RFT. The 356 sec which was used for RFT in scenario 1.3 achieves P_I value = 0.88 and P_E value = 0.859. The curve shows a better P_I value could be achieved if RFT is decreased, which will be seen in the next scenario 1.4.

4.5. Scenario 1.4: Attack via Route 1 with Decreasing Response Force Time. Results of the previous scenario and its analysis shown in Figure 10 are dictating a necessary solution to increase P_I by decreasing the RFT. Reviewing the geographical locations of the NPP in Figure 2, there is a possibility to relocate the Security Response Force Center from location #18 to location #26 which was assigned earlier to be Auxiliary Security Center. This will reduce the response force travel time to 300 sec as shown in Table 2 instead of the previous value of 365 sec in Table 1.

Assuming that PN will stay the same value of 0.995 and introducing the new value of RFT delay time = 300 sec to EASI program will produce a new value for $P_I = 0.927$ and $P_E = 0.922$ as shown in Figure 11, that is, crossing the P_E threshold value and being acceptable in this scheme.

4.6. Scenario 6.4: An Attack from Seaside. Referring to Figure 5, route 6 is the most critical route from the seaside. Scenario 6.4 is an attack through route 6, with consideration of all given recommendations in scenario 1.4. The coastal security includes the underwater sonar detection system and the underwater mesh fence as described in Section 3.3. The attack path action sequence and the security parameters PD, ADT, RFT, and PN are introduced to the EASI Program; the result is a value of $P_I = 0.937$ and $P_E = 0.932$. This result is indicating that the proposed security system will perform perfectly.

5. Results and Discussion

5.1. Effects of P_D on P_E. The previous discussion has pointed out that increasing P_D to the maximum possible available values in technology will maximize P_E to a certain limit, but it cannot individually raise P_E to the required value. The effect of increasing ADT is very vital because there is no usefulness of early detection without

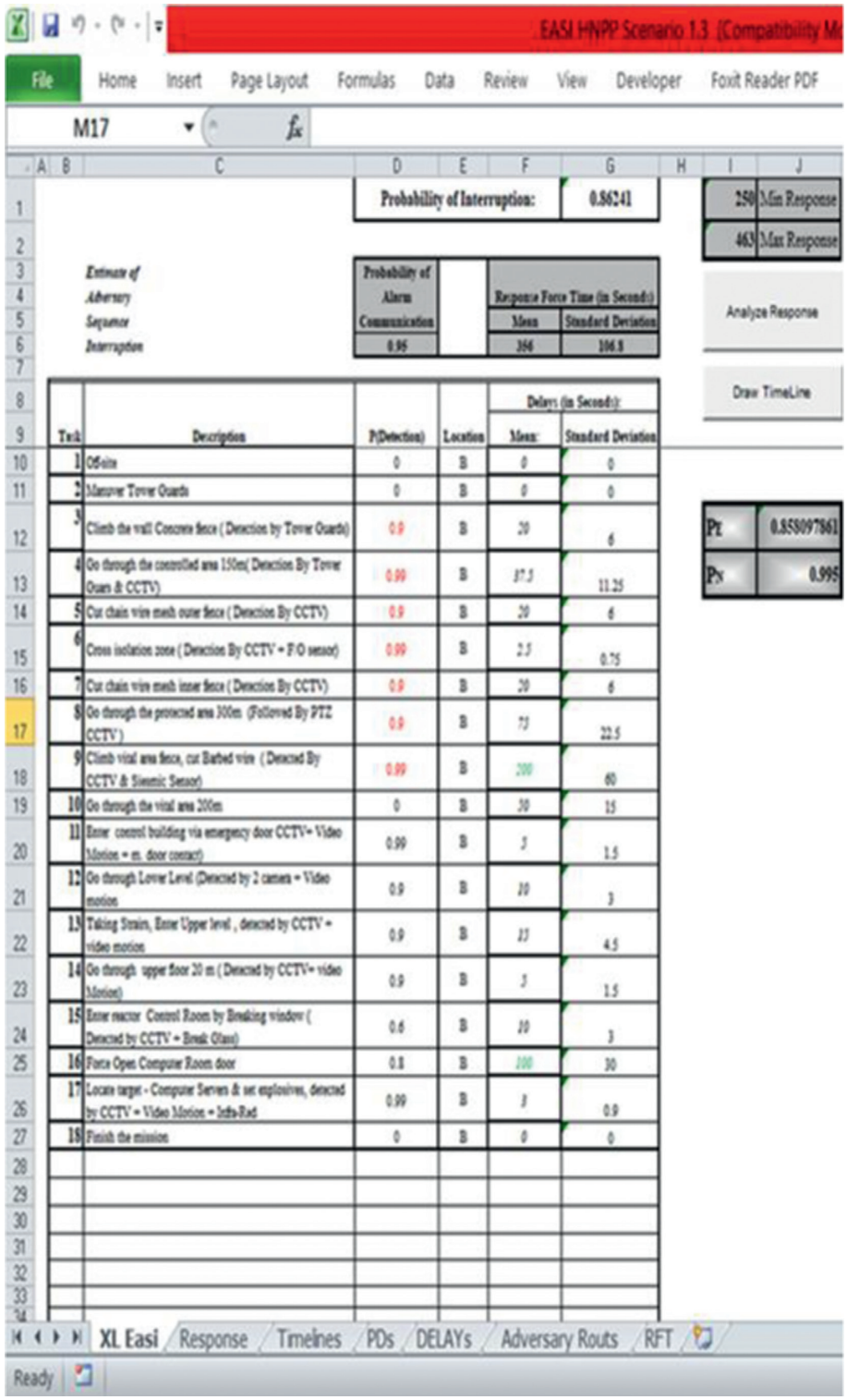

Figure 9: Attack path action sequence and EASI calculations of P_I and P_E for scenario 1.3, where P_E result = 0.858, increased, but still not acceptable.

having physical barriers to delay the adversaries until the arrival of response force. RFT value should be less than the ADT to allow the response force to arrive before the adversaries can finish their mission by hardening the physical barriers. Figure 12 illustrates P_I versus P_D for different scenarios, showing constant values of P_I with increasing P_D.

The constant value of P_I for each scenario means the detection function is completed if the detection is communicated to the command control center as early as

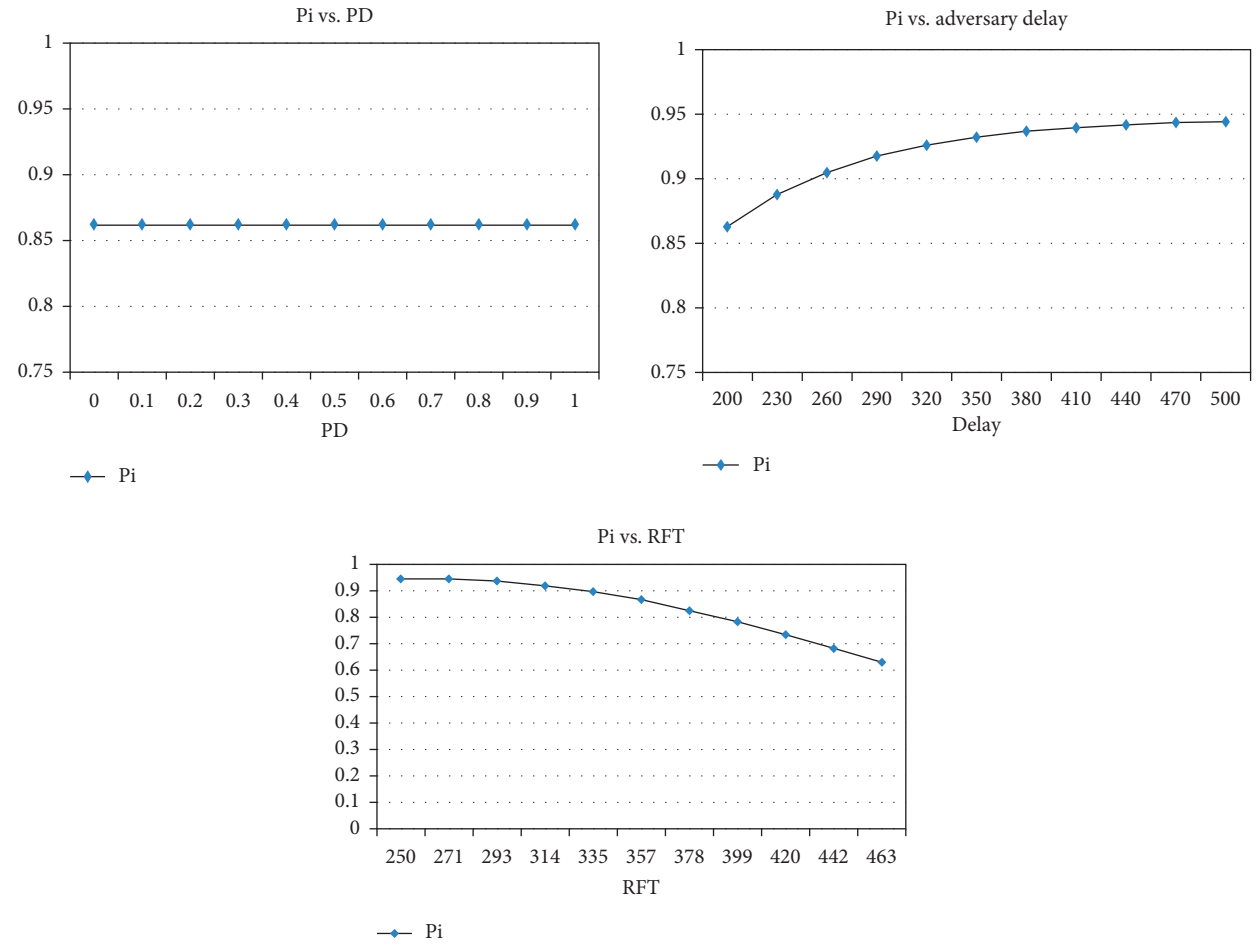

Figure 10: P_I versus P_D, ADT, and RFT separately for attack scenario 1.3.

Table 2: The response force travel time after relocation of response force center for scenario 1.4.

Guards delay time	Sec	Response force delay time	Sec
Alarm communication time	1	Alarm communication time	1
Alarm assessment time	45	Alarm assessment time	45
Communication time to guards	25	Communication time to guards	25
Guards preparation time	15	Response force preparation time	90
Guards travel and deployment time	34	Response force travel time (by vehicles); from nearer center	64
		On-site deployment time (after travel)	75
	120	Total RFT =	300

possible and fixed values of P_I and P_E are set. The next function of the security system is to delay the adversaries.

5.2. Effects of ADT on P_E. Figure 13 shows P_I versus ADT, for different scenarios, showing the proportional increasing contribution values of P_I with increasing ADT. This means that if the security system delay function is increased, the adversary mission will be more difficult to be completed. Increasing the ADT could be done by hardening physical barriers.

5.3. Effects of RFT on P_E. For the security system, to do its function, RFT should be less than ADT to allow the response force to combat with the intrusion event and neutralize the adversaries.

Figure 14 illustrates P_I versus RFT for different scenarios, showing increasing contribution values of P_I with decreasing RFT, which shows that RFT is having the most influencing factor of the security system.

RFT should be less than the ADT by enough time to allow neutralizing the adversaries. It should be taken into consideration that RFT is having a minimum value by nature.

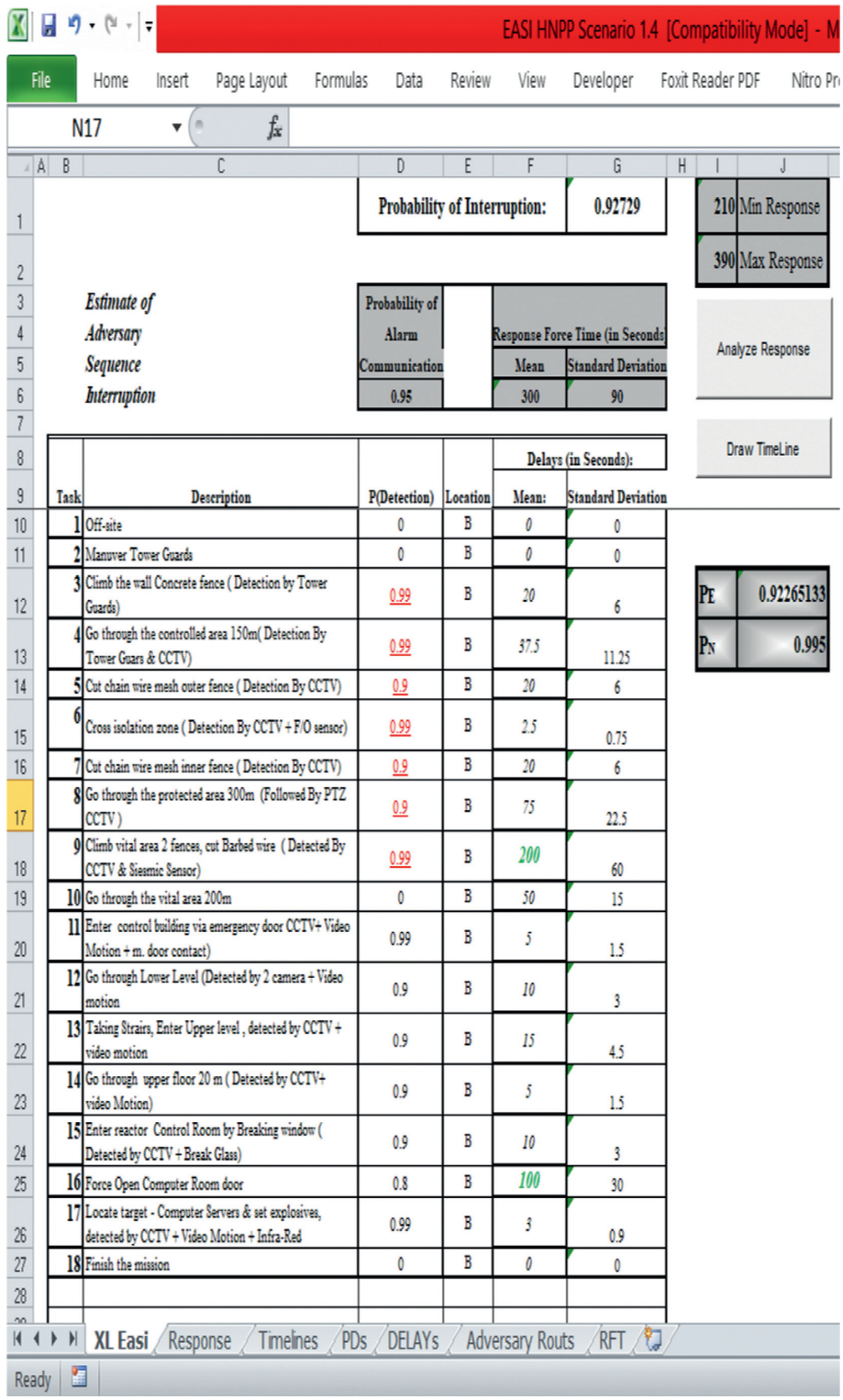

FIGURE 11: Attack path action sequence and EASI calculation of P_E for scenario 1.4, where P_E result = 0.922, increased and acceptable.

5.4. Risk vs P_E. Referring to the risk equation (2) in Section 4, Figure 15 illustrates P_E versus risk (R) for two scenarios 1.1 of the lowest P_E and 1.4 of the highest P_E, showing the reverse proportionality between risk and effectiveness P_E. The curves of P_E and risk in the y-axis are against RFT in the x-axis. The red vertical arrow is showing the critical RFT of 325 sec value which is still less than the ADT (573 sec). This RFT_{Crit} is required to gain the minimum acceptable value of P_E = 0.9 required to neutralize the adversaries.

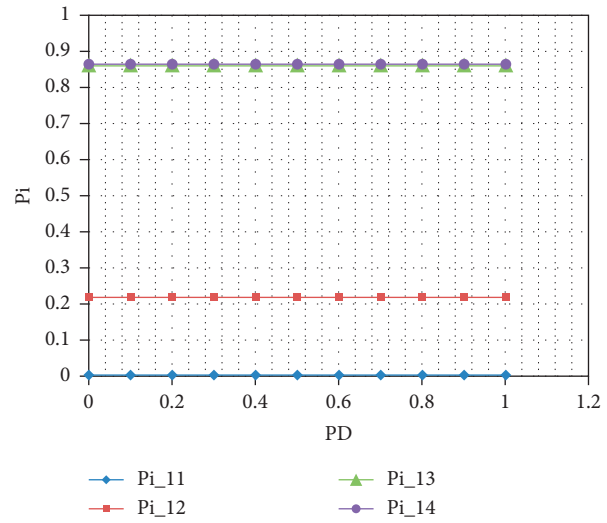

Figure 12: P_I versus PD for 4 scenarios, showing constant contribution values of P_I with changing P_D.

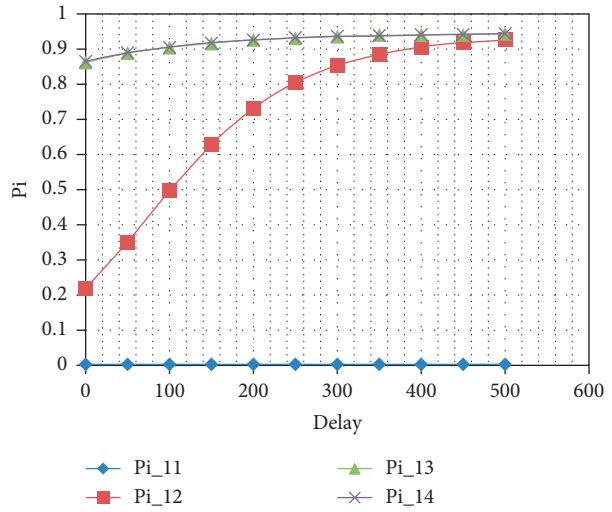

Figure 13: P_I versus ADT, for 4 scenarios, showing increasing contribution values of P_I with increasing ADT.

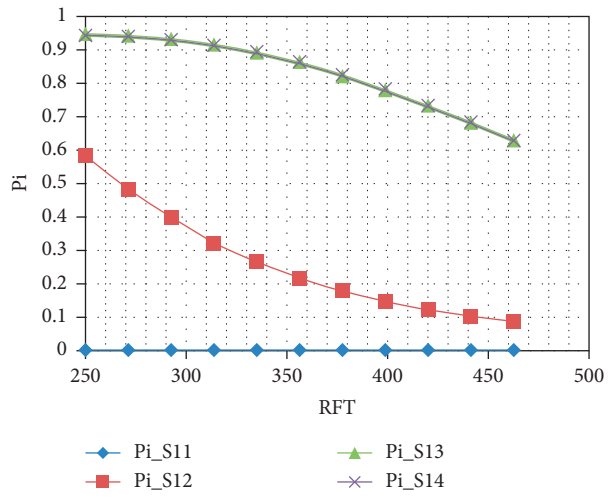

Figure 14: P_I versus RFT for 4 scenarios, showing increasing contribution values of P_I with decreasing RFT.

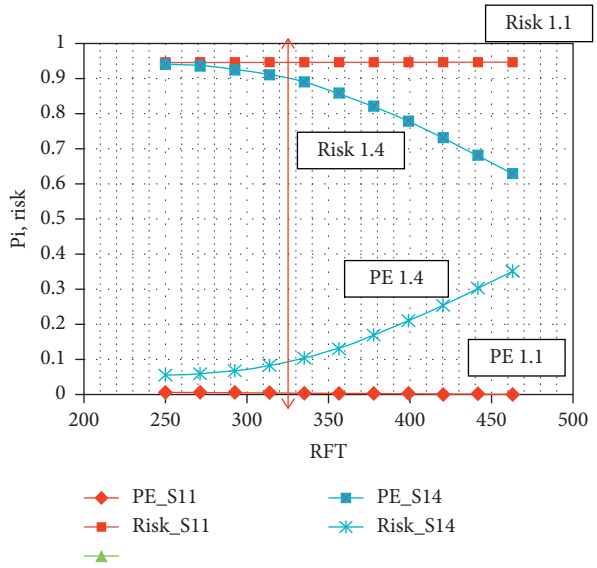

FIGURE 15: P_E versus risk for two scenarios 1.1 (the lowest P_E) and scenario 1.4 (the best P_E) shows the reverse relationship between risk and effectiveness probability P_E. The curves of P_E and risk are on the x-axis of the RFT.

6. Conclusion

After designing a physical electronic integrated security system (ISS) applied to a commonly structured commercial NPP, this paper is recommending the designers to use the proposed evaluation methodology for the proposed system and setting a threshold value for its $P_E = 0.9$ to achieve the security license. To achieve this, it is recommended that security system design should be embedded in the early NPP design and site planning stage accompanying the "Defense-in-Depth" (DID) principle. It is important to use modern detection devices which have the best detection probability factor from 0.98 up to 0.99. The evaluation process recommends also extending the adversary delay time and reducing the response force arrival time RFT to ensure a successful neutralization for any adversary.

Abbreviations

ADT: Adversary delay time
ASD: Adversary sequence diagram
ASSESS: Analytic system and software for evaluation of safeguards and security
CCTV: Closed circuit television
EASI: Estimate of adversary sequence interruption program
DID: Defense in depth
F/O: Fiber optic
HNP: Hypothetical nuclear power plant
IAEA: International atomic energy agency
IP: Internet protocol
ISS: Integrated security system
NPP: Nuclear power plant
P_D: Probability of detection
P_N: Probability of neutralization
P_E: Effectiveness probability
P_C: Probability of communication
PPS: Physical protection system
PSS: Physical security system
PTZ: Pan, tilt, and zoom
R: Risk
RFT: Response force travel time
SCC: Security Command Center
SD: Standard deviation
SLD: Single-line diagram
TCP/IP: Transmission control protocol/internet protocol
UWSS: Underwater sonar system.

Data Availability

The data used to support the findings of this study are described in the article and will be available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. L. Garcia, *Design & Evaluation of Physical Protection Systems*, Sandia National Laboratories, California, CA, USA, 2nd edition, 2008.
[2] B. Arnold, *A Scalable Systems Approach for Critical Infrastructure Security*, Sandia National Laboratories, California, CA, USA, 2002.
[3] K. Mark, *Security-By-Design Handbook*, Sandia National Laboratories & Japan Atomic Energy Agency, Tokyo, Japan, 2013.
[4] D. W. Whithead, C. S. Potter, and S. L. O'Connor, *NPP Security Assessment Technical Manual, SAND-007-5591*, Sandia National Laboratory, Albuquerque, NM, 2007.
[5] D. Hutter, *Physical Security and Why it Is Important*, SANS Institute, Maryland, MA, USA, 2016.
[6] IAEA, *Handbook of Physical Protection Systems Design for Nuclear Materials & Nuclear Facilities*, International Atomic Energy Agency, Vienna, AU, USA, 2017.
[7] W. Brueher, *Nuclear Security Assessment Methodology for Regulated Facilities*, IAEA, Vienna, AU, USA, 2016.
[8] IAEA, *Identification of Vital Areas at Nuclear Facilities, Technical Guidance*, Vol. 16, IAEA, Vienna, AU, USA, 2012.
[9] M. L. Garcia, *Vulnerability Assessment of Physical Protection Systems*, Publication of Sandia National Laboratories, California, CA, USA, 2005.
[10] A. A. saleh, "Physical protection evaluation process for nuclear facility via sabotage scenarios," *Alexandria Engineering Journal*, vol. 56, pp. 831–839, 2017.
[11] O. D. Oyeyinka, "Determination of system effectiveness for physical protection systems of a nuclear energy centre," *Science & Technology Journal*, vol. 4, pp. 8–16, 2014.
[12] T. ho Woo, "Systems thinking safety analysis: nuclear security assessment of physical protection system in nuclear power plants," *Science and Technology of Nuclear Installations*, vol. 2013, Article ID 473687, 5 pages, 2013.
[13] J. Zamanali and C. Chwasz, *Nuclear Power Plant Security Assessment Guide*, USNRC publications, Washington, DC, USA, 2013.

[14] 27th International Training Course, *Lone Pine, Hypothetical Facility Exercise Data Handbook*, 27th International Training Course, Albuquerque, New Mexico, USA, 2018.
[15] Rusatom, *VVER Manufacturing Co.), "The VVER Today, Evolution, Design& Safety" Manufacturer Brochure*, https://www.rosatom.ru/, 2020.
[16] Dynacorp, *Gurad Tower Manufacturer*, https://www.dynasystems.co.uk/dynatower, 2020.
[17] Pelco, *CCTV Product Overview Manufacturer Catalogue*, 2020.
[18] Manchester University, *Directorate of Estates Procedure and Information Manual EPM Pm26 – Standard CCTV Specification*, Manchester University, Manchester, UK, 2017.
[19] IP Video System Design Tool, *Lens Specification Calculation Program by JVSG in Website*, http://www.jvsg.com/cctv-lens-calculator/, 2020.
[20] *Architectural and Engineering Specification for Senstar Co.,White Paper Specifications for: "Fiber Optic Buried Intrusion Detection System"*, 2020.
[21] B. Co, *Advanced F/O Sensing Solutions, Product Manual*, 2020.
[22] ZHIBEI, *Anti-Corrosion PET Mesh Fence*, https://zhibeinetting.com/pet-netting/%2020.
[23] SAES, *Under Water Sonar Intrusion Detection System*, SAES Defense & Security Co., Spain, 2020.
[24] Z. Vintr and M. Vintr, *Evaluation of Physical Protection System*, IEEE International Carnahan Conference on Security Technology, India, 2012.
[25] SANDIA, 25th Training Course, *Chapter 18, "Adversary Sequence Diagram (ASD) Model*, SANDIA, 25th Training Course, Albuquerque, NM, USA, 2018.
[26] IAEA, Training Course, *Chapter 18 "Introduction to the Evaluation of Physical Protection Systems*, IAEA, Training, Vienna, AU, USA, 2018.